Network of Excellence

Deliverable D14.4

Report on Second industry research seminar and on ongoing standardization
Abstract

This deliverable reports on some of the most visible activities performed within WP 14, namely, a panel on quantitative aspects in security held within the 'Quantitative Aspects in Security Assurance workshop (QASA)’ co-located with the ‘European Symposium on Research in Computer Security (ESORICS)’; the NESSoS 2nd industry-research seminar held with the Annual Privacy Forum in Cyprus, and a report on standardization efforts performed by different NESSoS partners.

Keyword List

Security metrics, industry best practices, metric interpretation, ISO/IEC, standards, privacy, future internet
# Document History

<table>
<thead>
<tr>
<th>Version</th>
<th>Type of Change</th>
<th>Author(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>Structure</td>
<td>Marina Egea (ATOS)</td>
</tr>
<tr>
<td>0.2</td>
<td>Chapter 1</td>
<td>Marina Egea (ATOS)</td>
</tr>
<tr>
<td>0.3</td>
<td>Chapter 1 revised</td>
<td>Marina Egea (ATOS)</td>
</tr>
<tr>
<td>0.4</td>
<td>Chapter 2</td>
<td>Aljosa Pasic (ATOS)</td>
</tr>
<tr>
<td>0.5</td>
<td>Chapter 3</td>
<td>Aljosa Pasic (ATOS), Jorge Cuellar (Siemens),</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Benoit Baudry (INRIA), Pieter Philippaerts</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(KUL), Fabio Martinelli (CNR)</td>
</tr>
<tr>
<td>0.6</td>
<td>Chapter 1</td>
<td></td>
</tr>
<tr>
<td>0.6</td>
<td>Approved by internal reviewers</td>
<td></td>
</tr>
</tbody>
</table>
Table of Contents

LIST OF FIGURES ........................................................................................................ 7

1 INTRODUCTION ........................................................................................................ 9

2 PANEL: QUANTITATIVE ASPECTS IN SECURITY ASSURANCE (QASA 2012).
   SECURITY METRICS ................................................................................................ 11
   2.1 Panel participants ............................................................................................... 11
   2.2 Presentations ...................................................................................................... 13
   2.3 Conclusion of the panel ..................................................................................... 16

3 NESSoS 2ND INDUSTRY RESEARCH SEMINAR AT THE ANNUAL PRIVACY
   FORUM, CYPRUS, OCTOBER 10TH 2012 .............................................................. 17
   3.1 Description of presentations and discussions ..................................................... 17
   3.2 Conclusions ...................................................................................................... 19

4 STANDARDIZATION ACTIVITIES ......................................................................... 21
   4.1 Conclusion ........................................................................................................ 22

BIBLIOGRAPHY .......................................................................................................... 23
List of Figures

Figure 2.1: Workflow: Security assessment for products and solutions ........................................ 13

Figure 3.1: A4Cloud approach ........................................................................................................ 20
1 Introduction

D14.4 reports on some of the most visible activities performed within WP 14, namely, a panel on quantitative aspects in security held within the ‘Quantitative Aspects in Security Assurance workshop (QASA)’ co-located with the ‘European Symposium on Research in Computer Security (ESORICS)’; the NESSoS 2nd industry-research seminar held with the Annual Privacy Forum in Cyprus, and a report on standardization efforts performed by different NESSoS partners.

The main conclusion that could be drawn from the QASA panel is the increasing, verifiable need to further expand the research activities on quantitative aspects in security, being those aspects related to security metrics, service execution risks and economic revenue for service offering. Furthermore, from an industrial setting it was shown that there are several scenarios where fruitfully managing quantitative security aspects can lead to a competitive advantage.

From the NESSoS 2nd industry-research workshop held with the Annual Privacy Forum, we remark that software and service engineering researchers, as well as Future Internet community, are well aware of privacy concerns and the new risks that come from e.g. location privacy or superposing data coming from different devices. On the contrary, it is a relevant problem that we cannot argue the same for lawyers and policy makers that are not even aware of the inherent complexity of IT systems but frequently join privacy-by-design discussions. Thus, inputs and involvement from NESSoS community is necessary in order to increase stakeholders awareness and understanding of the complexity of this problem.

From the latter chapter, the report on standardization activities, we have identified the need of performing joint activities that can be promoted by the consortium as a whole in order to maximize our impact and defend NESSoS interests in selected standardization task forces.

The workshop Quantitative Aspects in Security Assurance (QASA 2012 - http://www.iit.cnr.it/qasa2012) was held in Pisa (Italy), the 14th of September of 2012. QASA is a workshop co-located with ESORICS and this year it has been sponsored by NESSoS. Within the QASA workshop program there was a panel on Quantitative Aspects of Security-Security Metrics, where various industrial and academic researches presented their ideas and participated in a discussion, including questions from the audience.

2.1 Panel participants

The list of participants was as follows: Jorge Cuellar (Siemens-Germany), Reijo Savola (VTT-Finland), John Favaro (INTECS), Lorenzo Strigini (University City of London), Ricardo Scandariato (KUL), and Marina Egea (ATOS). The panel was moderated by Fabio Martinelli (CNR).

Fabio Martinelli is a senior researcher of the National Research Council of Italy where he leads the interdepartmental security project. His research interests involve security and privacy in distributed and mobile systems and foundations of security and trust. He has been involved with several leading roles in the following FP6-FP7 projects: ARTIST2, BIONETS, CONTRAIL, CONNECT, CONSEQUENCE, GRIDtrust, NESSoS, S3MS, SESAMO, SENSORIA. He is active in community building efforts. He founded and managed the WG on security and trust management (STM) of the European Research Consortium in Informatics and Mathematics (ERCIM) since 2005 till 2009 and he is involved in several Steering Committees of international WGs or Conferences/workshops. In particular, he is the co-initiator of the International Workshop series on Formal Aspects in Security and Trust (FAST), one of the first events to recognize the necessity to consider trust and security issues altogether in new virtual and dynamic organizations/coalitions. Fabio Martinelli is also the coordinator of the EU project NESSoS and he is the co-chair of the Italian technological platform in homeland security (SERIT), both devoted to community building efforts.

Jorge Cuellar is a principal research scientist at Siemens AG. He was awarded the DI-ST Award for the best technical Achievement for his work on modelling of operating systems and transaction managers. He has co-authored about 30 papers on different topics, including mathematical modelling of performance analysis, on learning algorithms, hand-writing recognition, formal specification and verification of distributed system design, and security. He has done technical standardization work, related to the development of privacy and security protocols at the IETF, 3GPP, and the Open Mobile Alliance. He has worked in several EU funded research projects, in particular in AVISPA and AVANTSSAR, both related to the formal modelling and verification of security and currently in NESSoS, WebSand and SPACIoS. He has served in many Program Committees in international conferences, and in particular he has been the PC Co-Chair of SEFM (Software Engineering and Formal Methods in 2004), FM’08 (F ormal Methods in 2008), and STM’10 and in the steering committee of ESSoS. He has presented more than 20 invited talks at conferences and seminars, and acts regularly as a reviewer for international conferences and journals. He has been in the editorial board of Journal of Science of Computer Programming - Elsevier, and has been guest editor in several journals. He is a member of the Industrial Curatory Board of Dagstuhl, Leibniz Centre for Informatics, the world’s premier venue for informatics. He has held many short term visiting teaching positions, in different Universities around the world.

Reijo Savola received the degree of M.Sc. in Electrical Engineering (with honors) from the University of Oulu, Finland, 1992, and the degree of Licentiate of Technology in Computer Science from the Tampere University of Technology, Finland, 1995. He is currently working as a Senior Research Scientist and the Network and Information Security Research Coordinator of VTT Technical Research Centre of Finland. He has experience in information and network security, software engineering, telecommunications, multi-technology engineering topics and in digital signal processing algorithms. He has seven years of industrial experience in telecommunications sector, having worked as a software engineering and digital signal processing consultant for Elektrobit Group Plc. in Oulu, Finland and in Redmond, WA, United States. Mr. Savola acts as a member of Board of Advisors, Software Assurance Forum for Excellence in Code (SAFECode), as the chairman of the Finnish Standards Association (SFS) National Advisory Group.
for JTC1/SC27 (IT Security Techniques) of ISO/IEC Standardization, and as the chairman of the Security,
Trust and Dependability Working Group within the Expert Advisory Group of the eMobility European Tech-
nology Platform (ETP). He acts as a member of program committee and reviewer for various international
conferences with a focus on information security. He is an author of 60 research papers in this field.

His current research interests include security requirements engineering, security and trustworthiness
metrics development, security assurance methods and tools. His research interests are steered by the
vision that there is a strong need for bridging the gaps between information security, risk management
and security engineering. We need more systematic, built-in and industrial-strength methods and tools for
software-intensive and telecommunication systems development.

John Favaro got a computer science degree at Yale and the University of California at Berkeley in the
1970s and spent a couple of years as a research assistant at the Technical University of Munich.
In the 1980s, he worked for a few years in the telecommunications industry in Paris, and then for several
more years as a consultant in different areas of software engineering with a number of companies in
Germany. He participated in several initiatives of the European Commission during those years, including
the experts group on Software Engineering Environments, and the NATO Industrial Advisory Group. He
co-wrote a book on programming languages for robotics and first began to be interested in software reuse.
In the early 1990s he came to Italy to head the European Space Software Engineering Environment
project. At that time he began to be involved more deeply in the software reuse community and to par-
ticipate in the organization of the international conference on reuse. During that time he had done some
initial work on the economics of reuse, but in 1994 he began to investigate the economics of IT. In 1996
he began publishing on valuation techniques and their relevance for software engineers, culminating in an
approach called Value-Based IT Management (VBIM) in 1998. During that period, he continued to work
in software reuse, co-developing a methodology for domain analysis using extensions of elements from
the Unified Modeling Language.
Since 1998, he has been interested in agile methods and in particular the study of their characteristics
from an economic point of view.
Recently he has become involved with an initiative in the European Union to enable interoperability of
business and commerce registers throughout the Member States.
In January 2008 he took on a position as Associate Editor of IEEE Software magazine in the area of
software management.

Riccardo Scandariato received his PhD in Computer Science from Politecnico di Torino, Italy, in
2004. Since January 2006, he joined the Distributed Systems and Computer Networks Research Group
(DistriNet) at KU Leuven, Belgium. He is a permanent member of the staff (Research Expert, equivalent to
a lecturer) and he currently leads a team of security researchers in the area of secure software. Riccardo's
main research activities are in the area of secure software engineering, with a particular focus on empirical
methods in security (controlled experiments and mining software repositories) and security in software
architecture (principles, patterns and methods). He has been the Program Chair of the MetriSec workshop
in 2009 and 2010 and is currently a member of the Steering Committee.

Marina Egea is a Consultant Project Manager at Atos Research & Innovation (ARI), based in Madrid,
Spain. She holds a PhD in Computer Science from Universidad Complutense de Madrid (2008), a bach-
elor in Mathematics from the University of Granada (2001). After obtaining her doctoral degree, she
joined the Information Security Group at ETH Zurich as a postdoctoral researcher. In 2010 she moved to
IMDEA Software institute (Madrid) as a researcher. She has also participated in several R&D industrial
projects on modeling and validation of software systems. Her current interests include Secure Software
Engineering (NESSoS network of excellence), Secure Development of Trustworthy Composable Services
(Exploitation Manager of the ANIKETOS project), and Security Risk Analysis.

Lorenzo Strigini is currently the Director and Head of Centre or Software Reliability and Professor of
Systems Engineering at City University of London. He joined the Centre for Software Reliability in 1995.
He was previously a researcher with the Institute for Information Processing of the National Research
Council of Italy (IEI-CNR), and a visiting scientist at the University of California at Los Angeles and at the
Bell Communication Research Laboratories, Morristown. His research work has covered topics of fault-
tolerant design of computer hardware and software, of high-speed networking and of reliability and safety
evaluation. For IEI-CNR, he was the Principal Investigator on several projects, including the European
collaborative projects DELTA-4 (on the definition of a dependable, distributed computer architecture), PD-CS/PDCS2 (on the achievement and evaluation of dependability in computing systems) and SHIP (on assessing the effects of design faults on safety in industrial designs). Lorenzo Strigini has published numerous papers in international journals and conferences. He is a member of the IFIP Working Group 10.4 on Dependable Computing and Fault Tolerance.

### 2.2 Presentations

After the introduction to the panel, made by Fabio Martinelli (CNR) who coordinated the discussion, each speaker started to present his/her points of view/experience on the suggested topic of discussion.

**Jorge Cuellar** talked about Security Assurance Levels (SAL) and which check lists they used in Siemens to test them. However, the main concern he exposed was related to Security Assurance for systems. In particular, he exposed the problem of how to correlate SW Engineering, Business Workflows, etc., to Security Assurance. At least to obtain some guiding principles on how to design or architect dependable, secure systems, and what or when one should test or analyse them. Further, can we measure the methods, techniques and tools for developing, designing, maintaining, and upgrading critical systems to obtain security measures? Dependable Systems have many security dimensions in a given or unforeseeable environment: adaptability to face unpredictable changes in the environment, robustness, and attack-tolerance.

Since security is like icebergs: the problems you see are only the tip or, even worse, some security icebergs have no tip! We do not go for 100% security, nor even for 100% confident security measures, no 100% confidence on measures. And on top of that, the typical disclaimer is that an adequate assessment of a complex application and IT infrastructure is very time consuming.

Jorge also provided a figure (see Fig. 2.1) containing as a workflow designed towards facilitating security assessment for products and solutions.

Regarding Risk Assessment in iterative SDLs, he recommended a develop, compile & run approach.

**Step 1** Determine security requirements & business worst case scenarios.

---

**Figure 2.1: Workflow: Security assessment for products and solutions**
Step 2 Capture security overview of the application.
   Extract annotated data flow Diagram.
   Identify vulnerability indicators.

Step 3 Translate business workflows, environment and worst case scenarios to technical threats.

Step 4 Estimate likelihood of technical threats. Estimate risk for each business worst case scenario. If risk is too high:
   1. Reduce attack surface, or
   2. Improve estimation by

Step 5 choosing adequate tests,

Step 6 performing the tests.

Reijo Savola focused his presentation in Gaps and Biases in Building Security In. He raised the question about which are the fundamental measurement objectives and how do they related. Essentially, the first point he made is that security controls effectiveness are enabled by a-priori security control correctness and both together cooperate to achieving security control efficiency.

As a second point, he argued that although security cannot be measured as a universal property, indicators based on security requirements were possible and useful. In any case, these indicators have to take into account the specific characteristics of software systems:

- Complexity of software systems: all potential state transitions are not known.
- Uncertainty: it is hard to assess how likely are transitions between states.
- Non-stationarity: security risks can vary, even rapidly, over time.
- Limited observability: it is hard to observe, measure and to correctly detect all events.
- Maliciousness: security threat agents can be strategically intelligent.

Finally, he showed that visualization of threats and indicators of possible security weakness could help better than simply making and showing numbers for complex security metrics as plain aggregations.

John Favaro based his presentation on the approach and experience from the SESAMO project (Security and Safety Modeling). Ensuring both safety and security in complex systems is one of the greatest challenges facing the industry today, and the development of quantitative decision support criteria for evaluating safety and security trade-offs is a primary focus in SESAMO.

John discussed what is known as the ‘Hamming Distance’, i.e., the number of positions at which strings of information are different. While error correcting codes in safety-related systems try to maximize the Hamming Distance (to introduce as much redundancy as possible and recognize communication errors), cryptographic codes in security-related systems try to minimize the Hamming Distance (to equally distribute code words over the code space and protect change of information).

There a number of conflicts and challenges between security and safety. For instance, security relies on encryption & authentication, confidentiality, open trust model, up-to-date security patches, and extensive use of COTS. In contrast, safety relies on timeliness under severely restricted resources, redundancy, closed trust model, continuous operation through upgrades, and extensive use of proprietary systems.

SESAMO aims to define a rigorous model that enables joint reasoning about safety and security, thus the reasoning can be formulated in a model based way, in terms of model elements and properties. The next step for SESAMO would be to identify enabling mechanisms for safety and security and create building blocks from them. Building blocks must be accompanied by contextual analysis elements, with quantitative results. Without quantitative results, the enabling mechanisms of SESAMO are weakened for certification / accreditation.

Since, it is a premise of SESAMO that safety and security cannot always be reconciled in a perfect ‘win-win’ manner, the elaboration of decision support strategies is a natural consequence. To this regard, quantitative analysis results allow informed decision making.
Lorenzo Strigini talked about ‘Security, quantification and metrics: a view of application challenges.’ He first reported on his group background regarding security at the Centre for Software Reliability. This work included conceptual work on measure and prediction, empirical measurement of attacks, and security assessment of safety critical systems.

His reflection started stating that security metrics in lay terms still means a range of things, e.g., rigorous measures and probabilistic models often precious for insight even when not applicable to prediction, empirical measurement, empirical prediction systems, or management metrics. He also pointed out that application of quantitative methods in reliability and safety has a long history of successes, failures and mistakes, and still-open challenges which inspire reflections about security.

He argued that quantitative reasoning brings clarity but at a certain cost since the price of clarity is eternal vigilance, e.g. against the tempting, fallacious simplification, and against the simplistic use of the quantitative results. Also, he exposed that to tackle quantitative approaches one needs to build the big picture since numbers and quantitative formulas are part of a composite picture (a ‘case’), that needs to be built in such a way that it convinces if and only if it ought to be convincing. According to him, another gap that we needed to bridge is the one from quantitative results to decisions. For example, being given a correct description of risk does not imply using it correctly, though. He referred rich psychological literature (e.g., Kahnemann, ‘Thinking, fast and slow’) that showed that on the one hand, formal quantitative reasoning helps rational interpretation of raw facts and impressions but, on the other, its outputs new facts and impressions, with complex subtleties.

Riccardo Scandariato explained his group background on software security. He explained that in his team they were focus on prediction models for security vulnerabilities. Their target domain is represented by Android applications and they use machine learning techniques. The objective is to identify which parts of an application are likely prone to being vulnerable (and possibly a good target for further investigation). The main points highlighted by Riccardo were first, that as a research community, we need success stories in order to justify the introduction of new security-specific software metrics. Success stories already exist that leverage plain-old software metrics in order to assess security properties. The latter is a promising research direction. He explained that a way to foster success stories is to produce research results that can be replicated and repeated by third parties. To this aim, we should create open repositories, e.g., to share the data used in research papers.

Marina Egea started her discussion by introducing two definitions by the NIST document on ‘Directions on Security Metrics Research.’ According to this document, a security metric (or combination of security metrics) is a quantitative measure of how much of a security attribute or set of attributes an entity possesses. The problem she raised was focused on system security, in particular, which seems to be the weakest link, i.e., the end-user. As an illustration, she talked about a real problem in a big company like Atos. It is not rare the case when a business unit wants to receive a security certification. To get such certification employees are trained and monitored to test users’ awareness of security. Frequently, employees’ behaviour with respect to security when they handle confidential information (physically, digitally) is very important. For instance, if customer ask an Atos’ employee to send confidential information, should she send it? should she encrypt it? should she refuse? Of course, the size and distribution of this problem adds complexity. Atos has around 73,000 employees worldwide. Therefore she sustained that there should be a security research line focused on users since the role (and the satisfaction) of human beings in security is becoming more and more important (e.g. privacy), user-centered security policies should consider users’ choices regarding, e.g., dissemination of their personal information. But how can we measure that users’ choices are really met by the systems? Moreover, how can we know which is an end user’s expertise in IT security? How can we be sure that they understand their choices within a given application? or, shall we protect them since they do not really know what is going on?

And, at the end of the day if the system security gets violated: How can the impact of a security breach/information leak that exposes personal (confidential) data be objectively measured? How can the damage caused by revelation be repaired? If a user’s confidential data get to the cloud or to a third party, how can we ensure that all of them are removed under that user’s request?
2.3 Conclusion of the panel

From the panel discuss it has been clear that there is an increasing need to further expand the research activities on quantitative aspects in security, being those aspects related to security metrics, service execution risks and economic revenue for service offering. From an industrial perspective there are several scenarios where fruitfully managing quantitative security aspects can lead to a competitive advantage. We can learn lessons from the dependability community where such aspects has been mastered (although facing less unpredictable scenarios and rationale attackers). Still it is a challenge that the research community at large plans to address. Starting from these conclusions of the panel, as main event of the QASA workshop during ESORICS, the researchers committed to organize another edition of the QASA workshop at the next ESORICS event in UK.
The European Commission proposed in January 2012 a reform of EU’s data protection rules to strengthen on-line privacy rights. In parallel, many EU funded projects in ICT research are addressing privacy from different angles. In light of the above, the European Commission Directorate General for Communications Networks, Content and Technology (DG CONNECT), the European Network and Information Security Agency (ENISA) and the Department of Computer Science of the University of Cyprus organized a two day event with the objective to provide a forum to academia, industry and policy makers in the field. The event slogan was ‘closing the loop from research to policy’ and this clearly describes also the type of presentations and audience that attended: mix of policy makers and researchers from different domains and disciplines. Some outputs from this conference were used for public consultations on improving Network and Information Security in the EU, open until 12 October 2012 as well as for a short report on the conference for members of the Committee on Civil Liberties, Justice and Home Affairs (LIBE committee) at the European Parliament. In this respect we are happy that this report was also highlighting the main issues addressed during the NESSoS workshop.

The first presentation was done by Aljosa Pasic, the chairman of NESSoS industrial advisory board (IAB) and WP14 leader, who briefly introduced NESSoS project and its objectives, followed by a discussion on the need for abstractions and privacy policy assurance (Model Driven Privacy: does it exist?), as well as roles that model transformations could play. The second presentation by Jorge Cuellar, the vice-chairman of IAB titled ‘The need to standardize location privacy protection policies – A look at the IETF’. Claire Vishik (INTEL) talked about the ‘Principles of Privacy by Design in Smart metering: issues of importance to privacy engineers and technologists’, Slim Trabelsi (SAP) talk about the use of USDL-SEC [5] for privacy goals, and finally, Nick Wainwright (Hewlett Packard) talk about the need of accountability for the Cloud.

3.1 Description of presentations and discussions

The research has already addressed languages for privacy policy, but the hard problem of assurance that this policy is actually enforced remains open. We need some form of confidence that the ICT system managing data actually enforces privacy policies and it is sensible to divide assurance problem into areas of early (requirements, design phases) and late assurance (implementation and monitoring of operational environment). The most recent requirements engineering approaches consider security only at the technological level, failing to capture the high-level requirements of trust or privacy. There is a need for suitable abstractions and privacy research could look at other areas (e.g. model-driven security) for relevant issues. There is also a need for reasoning infrastructure, mappings and transformations (see [8] for an example of how to check security properties preservation through model transformations). While languages for model-based security (e.g., UMLSEc [4] and SecureUML [6]) provide support for integrating security requirement into system design models, there are no privacy ‘modeling’ languages at this abstraction level. Eventually, by reasoning about security/privacy very early we could study trade-offs, simulate policies and test protocols at a very early stage which would reduce overall cost for putting ‘privacy-by-design’ into practice. Policy transformation automation, for example, would generate low-level policy from e.g. natural language privacy requirements (and derived models). When a user is authenticated, then his/her identity and credentials are typically exposed as part of a security context. Some security systems might provide global access to security context while other will use control flow mechanisms to allow access to this context from service control points. When it comes to privacy and confidentiality services, rules that deal with what data is being accessed typically deal with data categories. For example, the Platform for Privacy Preferences (P3P [10]) defines standard categories including physical, health, demographic, and purchase. Defining service security rules in terms of categories or contexts is analogous to granting functional access to users based on their roles.

In NESSoS there is also a lot of ‘know-how’ on provide better support for capturing and incorporating security requirements, assurance protocols or on model-driven transformations. Rules can be combined into ‘process-like’ service coalitions and combinations in order to define what will be available to whom.
NESSoS - 256980

Abstract description of business service security characteristics enables on the consumer side to express customers (even when not security experts) to express their security requirements in a declarative way. An introduction to USDL-SEC is conceived as a means for expressing security features of services, described with USDL. A motivation for USDL-SEC introduction is to allow it provide means to compare and select services according to consumer needs. Among targets scenarios are cloud computing, service marketplaces etc. The Unified Service Description Language (USDL) is a platform-neutral language for describing services. The language is able to describe services from business to technical perspective and in and for clouds. The Unified Service Description Language (USDL) is a platform-neutral language for describing services. The language is able to describe services from business to technical perspective and in and for clouds. The Unified Service Description Language (USDL) is a platform-neutral language for describing services. The language is able to describe services from business to technical perspective and in and for clouds. The Unified Service Description Language (USDL) is a platform-neutral language for describing services. The language is able to describe services from business to technical perspective and in and for clouds. The Unified Service Description Language (USDL) is a platform-neutral language for describing services. The language is able to describe services from business to technical perspective and in and for clouds. The Unified Service Description Language (USDL) is a platform-neutral language for describing services. The language is able to describe services from business to technical perspective and in and for clouds.
certain security demands and find business services that comply with these demands. Service providers can use this specification to describe the security features of their services, and thus to support users in finding adequate alternatives to fulfil their needs. Three major requirements for this were explicit representation, machine readability and advanced composition support. In regard to privacy, so called Data Handler (DH) component that has been developed in FI-WARE project is a privacy-friendly attribute-based access/usage control system to (sensitive) data. Based on the sticky Policy mechanism, DH offers the possibility to attach privacy constraints directly to the data to facilitate the enforcement and the traceability. An enforcement engine is proposed to perform the access control decisions and the obligation executions (Retention period, usage notification, logging, etc.).

Increasing number of devices with precise positioning (GPS) and the fact that users consume services associated to their current position (e.g. through social platforms that encourage sharing of position) is one of the main challenges when it comes to privacy by design and secure service engineering. A method for obscuring location information has been described during one of the presentations. A location recipient is the entity that is given location about a target entity. The goal is to ensure that the recipient is unable to recover location information with better accuracy than is desired. There are several assumptions and many possible scenarios with many possible requirements that makes engineering particularly difficult.

In Smart Grid scenario (see, e.g. [7]) information could be shared without users knowledge or it could be intercepted. Usage data is often utilized without authorization and user awareness and it is also said that many privacy issues in smart meters and smart grid areas can be resolved or mitigated by technology solutions only. As mass deployments are anticipated, economic considerations will be important in establishing privacy friendly models. General privacy legislation can address issues relating to Smart Grid implicitly, and specific Smart Grid legislation or statute language is unnecessary. However, the development of Smart Grid infrastructure should follow the principles of Privacy By Design and Accountability, where privacy requirements are taken into account early on and throughout the development life-cycle and where entities take responsibility for the information they collect.

Finally, the challenges related to globalization and trust were also addressed in the workshop through A4Cloud project presentation. Globalization and new technologies like cloud are straining the traditional frameworks for privacy (e.g. model contracts, etc.). There is a need to increase trust at various levels (for consumers, clients and regulators) as well as the need to decrease regulatory complexity in global business environments, especially for cloud providers. Accountability can provide a clear and consistent framework of data protection rules and Accountability for the Cloud and other Future Internet Services (A4Cloud) is a new project that will address this issue through inter-disciplinary co-design framework depicted below.

### 3.2 Conclusions

Software and service engineering researchers, as well as Future Internet community, are well aware of privacy concerns and the new risks that come from e.g. location privacy or superposing data coming from different devices. The issue about privacy by design seems to be a relative vagueness when it comes to technical implementation (best practices for software and service engineers) as well as the management level priority where privacy by design might be seen as an unnecessary cost with no return on investment. One of the key challenges for service and software engineering community is articulating the test cases that involve multiple stakeholders and span over various domains, networks and services. The environment is rather dynamic (e.g. location privacy solutions that were good few years ago are not valid any more) and there could be research without short term return on investment. However, as one of the conference speakers commented ‘we have to move reference point’ and also to influence consumers and make them more aware about what privacy loss might mean in the future internet. Privacy by design discussions are very often attended by lawyers and policy makers that do not understand the complexity of software and service engineering process, so that lessons, inputs and involvement from NESSoS community is necessary.
Figure 3.1: A4Cloud approach
4 Standardization activities

Aljosa Pasic discussed the possibility of establishing a CWA (CEN workshop agreement) with the Austrian standard institute. This is a technical agreement, developed by an open workshop structure within the framework of CEN/CENELEC. It is CEN/CENELEC publication, the registered participants responsible for its contents. CWA does not represent the level of consensus and transparency required for a European Standard (EN), but is designed to offer market players a flexible and timely tool for achieving a technical agreement.

Results from NESSoS could contribute directly to the work program of the European Standardization Organizations and of the International Standards Organisations (ISO, IEC) through CWA. In addition here is the list of ongoing standardization activities related to cloud computing security (the meeting was about that topic actually):

ISO/IEC JTC 1 Information Technology, standards for cloud computing are developed within

- SC 7 Software and systems engineering
- SC 27 IT Security techniques

SC 38 Distributed application platforms and services

- ISO/IEC 20000-1 Information technology - Service management - Part 1: Service management system requirements
  - This management system standard for service management promotes the adoption of an integrated process approach to effectively deliver managed services to meet business and customer requirements
- ISO/IEC 20000-7 (in Development) Information technology - Service management - Part 7: Guidance on the application of ISO/IEC 20000-1 to the cloud
- ISO/IEC 19770 (several parts) Information technology - Software asset management
  - Particular requirements relevant to Cloud Computing are
    a) inventories of all installed software
    b) inventories of all entitlements
    c) mechanisms to determine all types of license usage
    d) key element of asset management in the cloud
- ISO/IEC 19793 Information technology – Open Distributed Processing – Use of UML for ODP system specifications
  - ODP standardization could support the characterization and description of Cloud Computing terms by use of (a subset of) the ODP viewpoints in an appropriate manner
  - Specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving formalized information security management systems (ISMS) within the context of the organization’s overall business risks
  - Control objectives and best practice controls to be used as implementation guidance
- ISO/IEC 27005 Information technology – Security techniques – Information security risk management
• guidance on implementing a process oriented risk management approach to assist in satisfactorily implementing and fulfilling the information security risk management requirements of ISO/IEC 27001

• ISO/IEC TS 27017 (WD) Information technology - Security techniques – Information security management - Guidelines on information security controls for the use of cloud computing services based on ISO/IEC 27002

• ISO/IEC 27018 (WD) Code of practice for data protection controls for public cloud computing services

• ISO/IEC 17788 (CD) Information Technology - Cloud Computing - Vocabulary

• ISO/IEC 17789 (WD) Information Technology - Cloud Computing - Reference Architecture

• ISO/IEC 17826 (FDIS) Information technology – Cloud Data Management Interface (CDMI)

Siemens has participated in the IETF for specifying the location privacy standard, and in the RFC 6772, that describes the language to express user’s privacy rules. These standard is currently in press [9].

During the past year, KUL has invested in the standardization front in two ways. In the field of security metrics, we are advocating the creation of open repositories where researchers can submit success stories with respect to software security metrics. New metrics can only be validated if the authors of a metric can reproduce the results of other researchers created by other authors. KUL is also investing a lot in web security, as described in D8.3. To this end, we are in direct contact with the W3C standardization body to modify existing and new standards with respect to security, and we are a research partner in the European Strategic Research Roadmap for European Web Security (STREWS) project [3].

In the last year, INRIA has participated in the standardization of the Common Variability Language (CVL) [2], which will be an essential asset to model adaptations of security policies and secure architecture. CVL provides a well-structured mechanism to express variability and to relate this variability to any model that conforms to the Meta-Object Facility [1]. The links to model-based assets can facilitate the derivation process, since that the choices in the variability level can be explicitly mapped to a realization layer and furthermore reflected in the assets level by means of executing a derivation algorithm. In this way, the CVL realization model works as an intermediate layer between the variability abstraction layer (can be seen as the features level) and the assets layer i.e., the set of model-based elements. Using variation points, this layer defines the set of modifications that must be executed over the set of base-model assets, according to selected features in the variability abstraction layer.

4.1 Conclusion

4.1 Conclusion

Given the difficulties and the long-term effort that is required to put in place a focused standardization effort, from NESSoS we are quite happy of the influence that we have had as a community during the last year. Individual partners have contributed to individual lines of standardization while ‘defending’ NESSoS interests. However, it is clear also that in the upcoming year there is a need of performing activities that can be promoted by the consortium as a whole in order to maximize our impact and defend NESSoS interests in selected standardization task forces.
Bibliography


